ANALISIS KEAMANAN JARINGAN PADA FASILITAS INTERNET (WIFI) TERHADAP SERANGAN PACKET SNIFFING

Makalah

Program Studi Teknik Informatika

Fakultas Komunikasi dan Informatika

Diajukan oleh :

Nama : *Bayu Arie Nugroho*

Pembimbing I : *Dr. Heru Supriyono, M.Sc.*

Pembimbing II : *Jan Wantoro, S.T.*

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS KOMUNIKASI DAN INFORMATIKA

UNIVERSITAS MUHAMMADIYAH SURAKARTA

Oktober, 2012

HALAMAN PENGESAHAN

Publikasi Ilmiah dengan judul :

"ANALISIS KEAMANAN JARINGAN PADA FASILITAS INTERNET (WIFI) TERHADAP SERANGAN PACKET SNIFFING"

Yang dipersiapkan dan disusun oleh :
Bayu Arie Nugroho
L200080076

Telah disetujui pada :

Hari : Jumat

Tanggal : 2 November 2012

2-11-2012 Pembimbing I

Dr. Heru Supriyono, M.Sc.

NIK : 970

Pembimbing II

Jan Wantoro, S.T.

NIK: 200.1304

Publikasi ilmiah ini diterima sebagai salah satu persyaratan

untuk memperoleh gelar sarjana

Tanggal 2-12-2012

Mengetahui,

Ketua Program Studi

Teknik Informatika

UNIVERSITAS MUHAMMADIYAH SURAKARTA
JURUSAN TEKNIK INFORMATIKA
FAKULTAS KOMUNIKASI & INFORMATIKA

Dr. Heru Supriyono, M.Sc.

NIK : 970

ANALISIS KEAMANAN JARINGAN PADA FASILITAS INTERNET (WIFI) TERHADAP SERANGAN PACKET SNIFFING

Bayu Arie Nugroho, Heru Supriyono, Jan Wantoro

Teknik Informatika, Fakultas Komunikasi dan Informatika

Universitas Muhammadiyah Surakarta

Email : bayuarienugroho@yahoo.co.id

Abstract :

Computer networks have two data transmission medium that is both wired and wireless. PT. Angkasa Pura I International Airport Adi Sumarmo Surakarta is one of the state-owned enterprises which have facilities wireless network (wifi). Wifi networks are particularly vulnerable to the threat of attack, because it's going to be open communication. A good security system is a needed in order to maintain the security of user data in order to avoid attacks by people who are not responsible. This study discusses the evaluation of the level of security wifi facilities in PT. Angkasa Pura I International Airport Adi Sumarmo Surakarta using netstumbler applications, inSSIDer and ettercap. NetStumbler is wifi hacking tools used to detect and identify an open wireless signal. inSSIDer is a free alternative that works exactly the same with netstumbler. Ettercap is a packet sniffer tool used to analyze network protocols and network security audit, which also has the ability to block traffic on the LAN network, steal passwords, and wiretapping active against common protocols. In this research done in two stages, the first to identify the presence and use of security wifi used inSSIDer software. The second phase of an attack packet sniffing using ettercap software security testing as a step in the PT. Angkasa Pura I International Airport Adi Sumarmo Surakarta. The results of this study are the detection of the presence and open wifi security or without security and recorded username and password. This can jeopardize the security of the user data traffic wifi network or wired LAN especially the employees, so that the necessary increase in security was good to be able to prevent / deal with packet sniffing attacks and more advanced.

Keywords: network security, packet sniffing, ettercap, netstumbler, inSSIDer.

Abstrak :

Jaringan komputer mempunyai dua media transmisi data yaitu kabel dan nirkabel. PT. Angkasa Pura I Bandar Udara Internasional Adi Sumarmo Surakarta merupakan salah satu Badan Usaha Milik Negara (BUMN) yang mempunyai fasilitas jaringan nirkabel (wifi). Jaringan wifi sangat rentan terhadap ancaman serangan, karena komunikasi yang terjadi bersifat terbuka. Diperlukan system pengamanan yang baik untuk dapat menjaga keamanan data pengguna agar

terhindar dari serangan yang dilakukan oleh orang–orang yang tidak bertanggung jawab. Penelitian ini membahas evaluasi tingkat keamanan fasilitas wifi di PT. Angkasa Pura I Bandar Udara Internasional Adi Sumarmo Surakarta dengan menggunakan aplikasi netstumbler, inSSIDer dan ettercap. Netstumbler adalah tools wifi hacking yang digunakan untuk mendeteksi dan mengidentifikasi sinyal wireless yang terbuka. inSSIDer adalah software alternatif yang fungsinya sama persis dengan netstumbler. Ettercap adalah tools packet sniffer yang dipergunakan untuk menganalisa protokol jaringan dan mengaudit keamanan jaringan, yang juga memiliki kemampuan untuk memblokir lalu lintas pada jaringan LAN, mencuri password, dan melakukan penyadapan aktif terhadap protokol-protokol umum. Dalam penelitian ini dilakukan dua tahap, yang pertama mengidentifikasi keberadaan dan keamanan wifi yang dipakai menggunakan software inSSIDer. Tahap kedua melakukan serangan packet sniffing menggunakan software ettercap sebagai langkah pengujian keamanan di PT. Angkasa Pura I Bandar Udara Internasional Adi Sumarmo Surakarta. Hasil dari penelitian ini adalah dengan terdeteksinya keberadaan dan keamanan wifi yang terbuka atau tanpa pengamanan dan terekamnya username dan password. Hal ini dapat membahayakan keamanan lalulintas data para pengguna jaringan wifi maupun LAN kabel khususnya para karyawan/i, sehingga diperlukan peningkatan keamanan yang baik untuk dapat mencegah/menangani serangan packet sniffing dan yang lebih lanjut.

Kata kunci : keamanan jaringan, packet sniffing, ettercap, netstumbler, inssider.

I. PENDAHULUAN

Pada saat ini *issue* keamanan jaringan menjadi sangat penting dan patut untuk diperhatikan, jaringan yang terhubung dengan internet pada dasarnya tidak aman dan selalu dapat diekploitasi oleh para *hacker*, baik jaringan *wired LAN* maupun *wireless LAN*. Pada saat data dikirim akan melewati beberapa terminal untuk sampai tujuan berarti akan memberikan kesempatan kepada pengguna lain yang tidak bertanggung jawab untuk menyadap atau mengubah data tersebut. Dalam pembangunan perancangannya, sistem keamanan jaringan yang terhubung ke Internet harus direncanakan dan dipahami dengan baik agar dapat melindungi sumber daya yang berada dalam jaringan tersebut secara efektif dan meminimalisir terjadinya serangan oleh para *hacker.*

Ettercap adalah *tools packet sniffer* yang dipergunakan untuk menganalisa protokol jaringan dan mengaudit keamanan jaringan. Ia memiliki kemampuan untuk memblokir lalu lintas pada jaringan *LAN*, mencuri password, dan melakukan penyadapan aktif

terhadap protokol-protokol umum. Sedangkan *Netstumbler* adalah *tools wifi hacking* yang digunakan untuk mendeteksi dan mengidentifikasi sinyal *wireless* yang terbuka dan menyusup ke dalam jaringan.

PT. (Persero) Angkasa Pura I merupakan salah satu Badan Usaha Milik Negara (BUMN) dalam lingkungan Departemen Perhubungan yang bergerak dalam bidang perhubungan udara khususnya penyedia jasa penerbangan udara. Wilayah kerja PT. (Persero) Angkasa Pura I meliputi sebagian besar bandara-bandara di kawasan timur Indonesia, sedangkan kawasan barat Indonesia pengaturannya ditangani oleh PT. (Persero) Angkasa Pura II. Manajemen Bandara Adisumarmo Surakarta berada dalam wilayah kerja PT. (Persero) Angkasa Pura I Bandar Udara Internasional Adisumarmo Surakarta.

Saat ini PT. Angkasa Pura I cabang Bandar Udara Internasional Adi Sumarmo telah menerapkan jaringan komputer kabel maupun nirkabel sebagai media pertukaran data/informasi pelayanan umum atau komersial, kepegawaian dan informasi penting lainnya. Terdapat dua jaringan yang terpasang dalam lingkup Bandara Adi Sumarmo yaitu :

1. Terinstall pada gedung baru yang di dalamnya terdapat ruang/kantor TU, Kasir, Administrasi, Pelayanan Umum dan KesKam dengan menerapkan jaringan kabel.

2. Terinstall pada Kantor TelNav yang terhubung dengan terminal bandara yang dengan menerapkan jaringan kabel dan terdapat dua access point sebagai jaringan nirkabel.

II. TINJAUAN PUSTAKA DAN LANDASAN TEORI

2.1. Telaah Penelitian

Menurut Thomas Setiawan (2004), pada penelitian dengan judul Analisis Keamanan Jaringan Internet Menggunakan *Hping, Nmap, Nessus, dan Ethereal*, yang berisi bahwa Sistem keamanan jaringan komputer yang terhubung ke Internet harus direncanakan dan dipahami dengan baik agar dapat melindungi sumber daya yang berada dalam jaringan

tersebut secara efektif. Apabila ingin mengamankan suatu jaringan maka harus ditentukan terlebih dahulu tingkat ancaman yang harus diatasi, dan resiko yang harus diambil maupun yang harus dihindari.

Penelitian lain yang dijadikan acuan adalah penelitian Aji Supriyanto (2006) dengan judul Analisis Kelemahan Keamanan Pada Jaringan *Wireless*, isi dari penelitiannya adalah Pemakaian perangkat teknologi berbasis *wireless* pada saat ini sudah begitu banyak, baik digunakan untuk komunikasi suara maupun data. Karena teknologi *wireless* memanfaatkan frekwensi tinggi untuk menghantarkan sebuah komunikasi, maka kerentanan terhadap keamanan juga lebih tinggi dibanding dengan teknologi komunikasi yang lainnya. Berbagai tindakan pengamanan dapat dilakukan melalui perangkat komunikasi yang digunakan oleh *user* maupun oleh operator yang memberikan layanan komunikasi. Kelemahan jaringan *wireless* secara umum dapat dibagi menjadi 2 jenis, yakni kelemahan pada konfigurasi dan kelemahan pada jenis enkripsi yang digunakan. Secara garis besar, celah pada jaringan *wireless* terbentang di atas empat *layer* di mana keempat lapis tersebut sebenarnya merupakan proses dari terjadinya komunikasi data pada media *wireless*. Keempat lapis tersebut adalah lapis fisik, lapis jaringan, lapis user, dan lapis aplikasi. Model-model penanganan keamanan yang terjadi pada masing-masing lapis pada teknologi *wireless* tersebut dapat dilakukan antara lain yaitu dengan cara menyembunyikan *SSID*, memanfaatkan kunci *WEP*, *WPA-PSK* atau *WPA2-PSK*, implementasi fasilitas *MAC filtering*, pemasangan infrastruktur *captive portal*.

Berdasarkan penelitian terdahulu yaitu penelitian dari Hendri Noviyanto (2011) dengan judul Analisis Keamanan Wireless di Universitas Muhammadiyah Surakarta yang berisi tentang pemakaian pemakaian access point yang mudah, bisa disembarang tempat yang terjangkau sinyal *wireless* tanpa harus berada disebuah tempat tertentu untuk dapat mengakses internet. Dalam penerapanya *wireless* menggunakan gelombang radio untuk saling

berkomuikasi atau bertukar informasi dari point ke point yang lain, sehingga jaringan tersebut sangat rawan dari serangan para penjahat dunia maya. Kondisi tersebut ditambah para pemula yang memasang access point untuk *hostpot* tanpa sepengetahuan yang berwenang, karena kurangnya pengetahuan sebuah *access point* tersebut dipasang tanpa pengamanan dan hanya bergantung pada settingan dari *vendor*.

2.2. LANDASAN TEORI

2.2.1. Konsep keamanan jaringan

Issue keamanan jaringan sangat penting dan patut untuk diperhatikan. Jaringan yang terhubung dengan internet pada dasarnya tidak aman dan selalu dapat diekploitasi oleh para *hacker*, baik jaringan *LAN* maupun *Wireless.* Pada saat data dikirim akan melewati beberapa terminal untuk sampai tujuan berarti akan memberikan kesempatan kepada pengguna lain yang tidak bertanggung jawab untuk menyadap atau mengubah data tersebut. Dalam pembangunan perancangannya, sistem keamanan jaringan yang terhubung ke Internet harus direncanakan dan dipahami dengan baik agar dapat melindungi sumber daya yang berada dalam jaringan tersebut secara efektif dan meminimalisir terjadinya serangan oleh para *hacker.*

Apabila ingin mengamankan suatu jaringan maka harus ditentukan terlebih dahulu tingkat ancaman yang harus diatasi, dan resiko yang harus diambil maupun yang harus dihindari. Berikut ini akan dibahas mengenai ancaman , kelemahan, dan *policy* keamanan jaringan.

2.2.2. Jenis - Jenis Ancaman Keamanan Jaringan

i. Packet sniffer

Packet sniffer adalah sebuah metode serangan dengan cara mendengarkan seluruh paket yang lewat pada sebuah media komunikasi, baik itu media kabel maupun nirkabel. Setelah paket-paket yang lewat itu didapatkan, paket-paket tersebut kemudian disusun ulang sehingga data yang dikirimkan oleh sebuah pihak dapat dicuri oleh pihak yang tidak berwenang. Hal ini dapat dilakukan karena pada dasarnya semua koneksi ethernet adalah koneksi yang bersifat broadcast, di mana semua host dalam

sebuah kelompok jaringan akan menerima paket yang dikirimkan oleh sebuah host. Cukup sulit untuk melindungi diri dari gangguan ini karena sifat dari packet sniffing yang merupakan metode pasif (pihak penyerang tidak perlu melakukan apapun, hanya perlu mendengar saja).

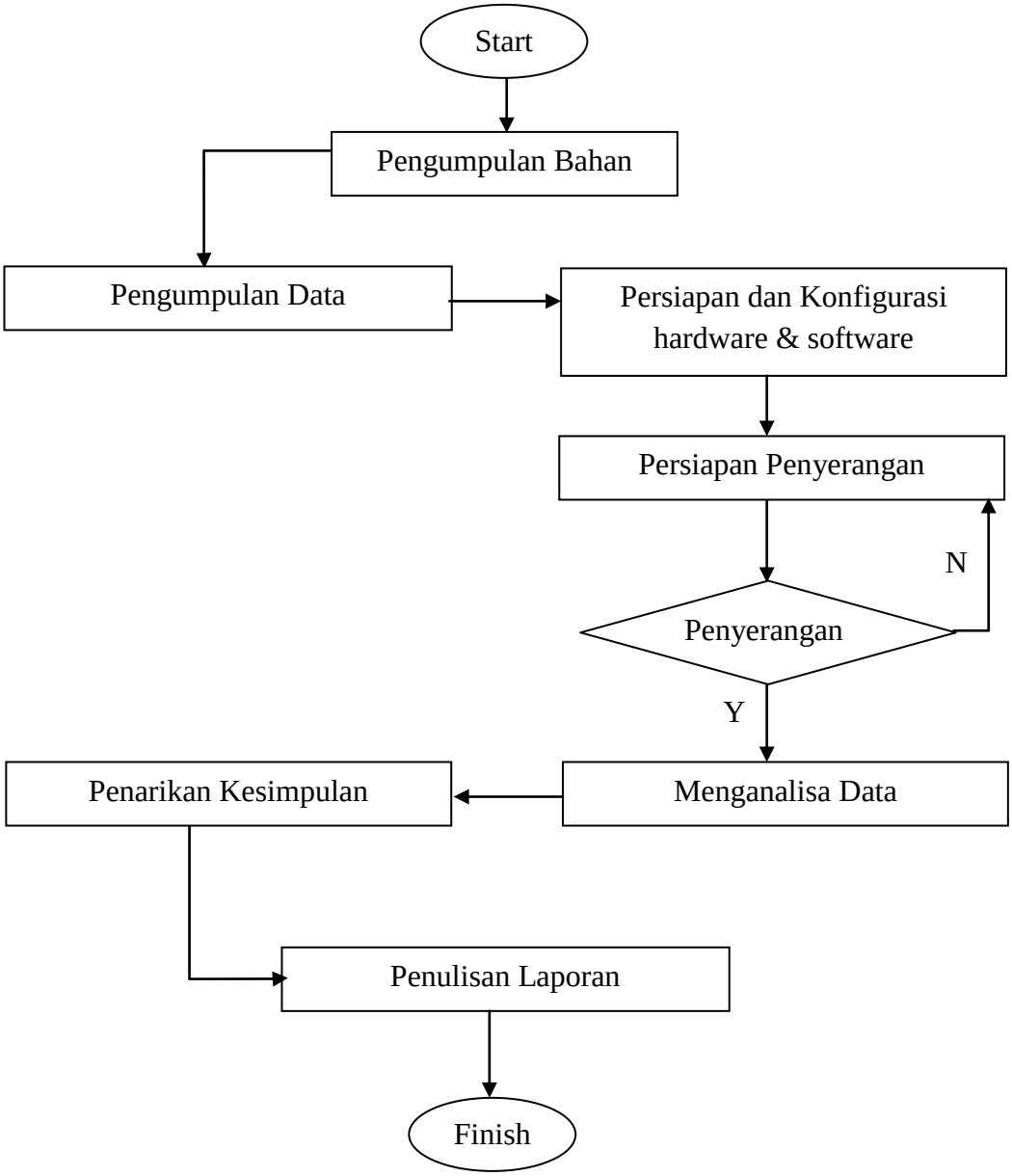
ii. ARP spoofing / ARP poisoning

ARP (Address Resolution Protocol) poisoning ini adalah suatu teknik menyerang pada jaringan komputer lokal baik dengan media kabel atau *wireless*, yang memungkinkan penyerang bisa mengendus *frames* data pada jaringan lokal dan atau melakukan modifikasi *traffic* atau bahkan menghentikan *traffic*. *ARP spoofing* merupakan konsep dari serangan penyadapan diantara terhadap dua mesin yang sedang berkomunikasi atau yang disebut dengan *MITM* (*Man in The Middle Attack)*. Prinsip serangan *ARP poisoning* ini memanfaatkan kelemahan pada teknologi jaringan komputer itu sendiri yang menggunakan *arp broadcast*. *ARP* berada pada layer 2, dimana alamat pada layer dua adalah *MAC address*. Misalnya sebuah host (contoh: PC) yang terhubung pada sebuah *LAN* ingin menghubungi *host* lain pada *LAN* tersebut, maka dia membutuhkan inforamsi *MAC address* dari *host* tujuan.

III. METODE PENELITIAN

3.1. Kerangka Pemikiran dan Flowchart

Dalam menjelaskan sebuah permasalahan kerangka pemikiran atau alur penelitian disajikan untuk mempermudah pemahaman dalam penelitian tersebut. Metode tersebut tersaji dalam diagram alir penelitian.



Gambar 3.1. Diagram Alir Penelitian.

Sesuai dengan diagram alir penelitian diatas penelitian ini dilakukan dalam beberapa tahapan.

a. Menyiapkan literatur, buku-buku, ebook dan artikel untuk menunjang penelitian.
b. Memenuhi persyaratan/prosedur perizinan penelitian yang diberikan oleh pihak KesKam (Keselamatan dan Keamanan) di PT. Angkasa Pura I Bandar Udara Internasional Adi Sumarmo, karena tidak semua tempat/lokasi boleh masuk kecuali karyawan tertentu yang berhak.

c. Mencari informasi data-data yang ada, konfigurasi jaringan kabel *LAN* dan *wifi* yang terpasang di seluruh lingkup Bandara Internasional Adi Sumarmo meliputi tempat, SSID, BSSID, enkripsi yang digunakan, channel.
d. Menyiapkan *hardware* dan *software* yang dibutuhkkan untuk menunjang pelaksanaan penelitian.
e. Melangkah untuk melakukan sebuah percobaan penyerangan kepada jaringan kabel *LAN* dan *wifi* untuk mendapatkan informasi tentang keamanannya.
f. Menarik kesimpulan untuk memutuskan sebuah saran yang bisa digunakan untuk mengamankan jaringan kabel *LAN* dan *wifi* melihat dari sisi pengguna.

3.2. Teknis Pengujian Keamanan

Pengujian keamanan bertujuan untuk memperoleh kesadaran akan permasalahan keamanan pada jaringan kabel dan nirkabel (*wireless LAN).*

a. Penulis mencoba mengidentifikasi keberadaan dan keamanan yang digunakan *wifi* target dengan menggunakan *software inSSIDer*.
b. Setelah mengetahui keberadaan dan keamanan yang digunakan *wifi* target, penulis masuk untuk mendapatkan koneksi dengan *wifi* target.
c. Langkah pengujian keamanan, setelah mendapatkan koneksi dengan *wifi* target, penulis mencoba melakukan serangan *Packet Sniffing* terhadap *wifi* dan jaringan kabel dengan menggunakan *software ettercap*, serangan akan berhasil jika transfer data tidak dilindungi oleh keamanan seperti SSL, IPSec, WEP, WPA dan WPA2. Karena data yang didapat terenkripsi.

IV. HASIL DAN PEMBAHASAN

4.1. Hasil Penelitian

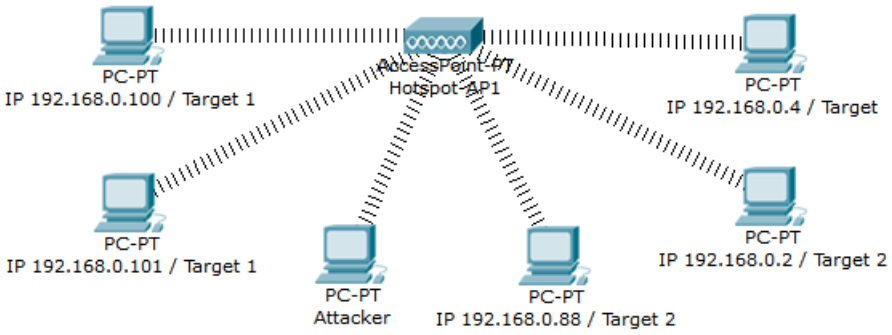
a. Mengidentifikasi Wifi

Percobaan ini dilakukan untuk mengidentifikasi keberadaan *wifi* dalam bentuk informasi lengkap dengan nama SSID, *mac address*, RSSI, *vendor*, *channel* yang dipakai, *network type* dan *security* atau keamanan yang digunakan. Hal ini dilakukan untuk memudahkan penyerangan untuk mendapatkan koneksi

dengan jaringan *wifi* yang ada. Dalam percobaan ini penulis mendapatkan *wifi* yang berada di area bandara tidak berpengaman / open.

b. Packet Sniffing

Percobaan ini dilakukan untuk mendapatkan informasi penting mengenai *account username, password,* akses DNS yang dituju dan informasi lain. Hal ini dimaksudkan agar penyerang dapat melakukan pengaksesan internet secara tidak sah demi keuntungan pribadi yang dapat mengakibatkan kerugian pada pengguna yang berada dalam jaringan. Pada percobaan ini, berhasil diperoleh informasi mengenai akses DNS yang dituju dan penulis juga mendapatkan username dan *password email* dari salah satu target. Dengan demikian, penulis dapat menyatakan tidak aman karena semua kegiatan dapat dengan mudah terekam dan mudah dicuri.

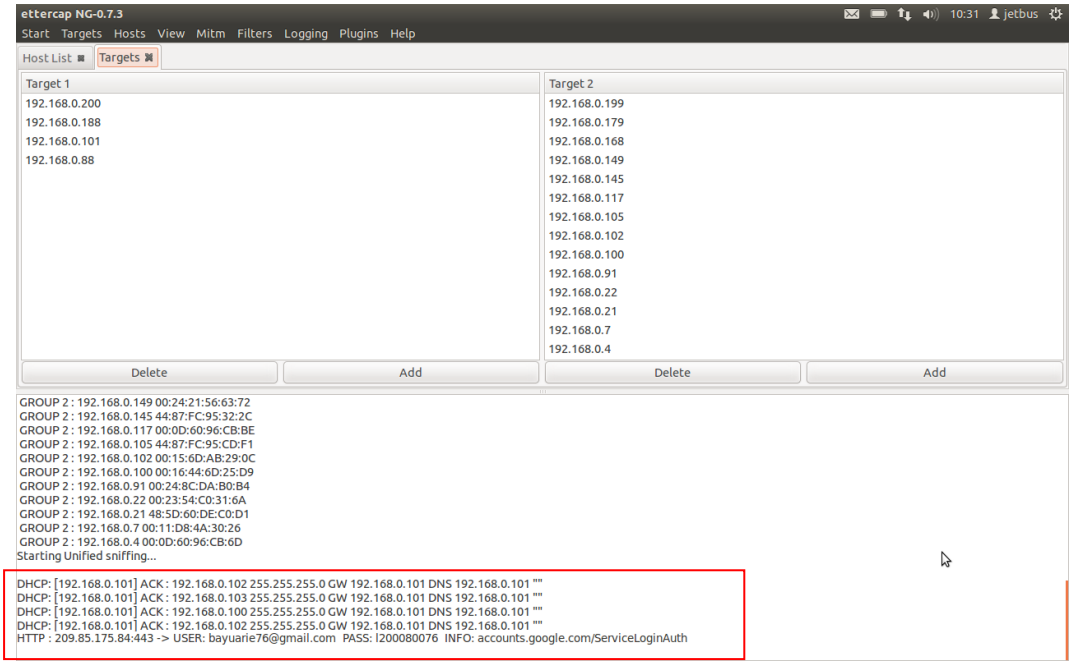


Gambar 4.1. Tampilan simulasi penyerangan.

Gambar diatas adalah gambaran skenario dimana attacker melakukan penyerangan dengan mengelompokkan target menjadi dua kelompok yaitu target 1 dan target 2 yang dimana berfungsi ketika target utama atau target 1 tidak melakukan aktifitas maka penyeangan akan berpindah pada target 2 begitu pula sebaliknya hingga attacker dapat merekam semua aktifitas yang berjalan.

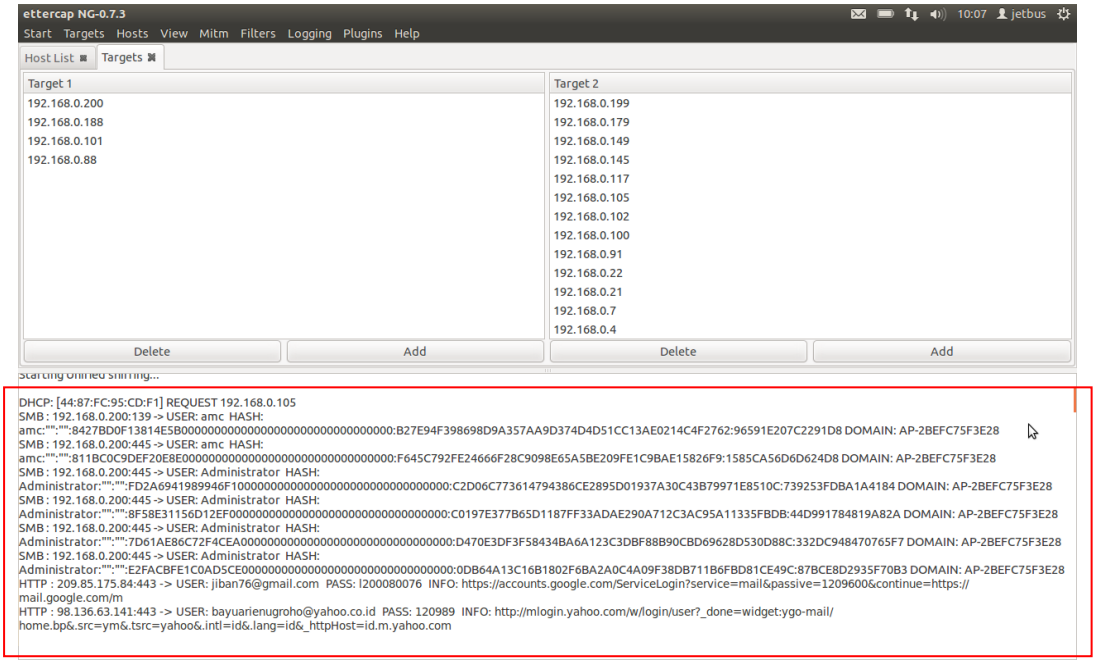
Karena dalam penelitian selama beberapa kali dalam jam kerja penulis tidak menemukan aktifitas yang mengakses akun dan password, penulis melakukan dua skenario yaitu :

a. Skenario pertama dengan langkah sebagai berikut :
   1. Penulis membuat beberapa akun dan password baru.
   2. Akun di coba login menggunakan komputer kantor.
   3. Penulis merekam aktifitas yang terjadi menggunakan software ettercap.



Gambar 4.2. Hasil penyerangan Packet Sniffing pada wifi.

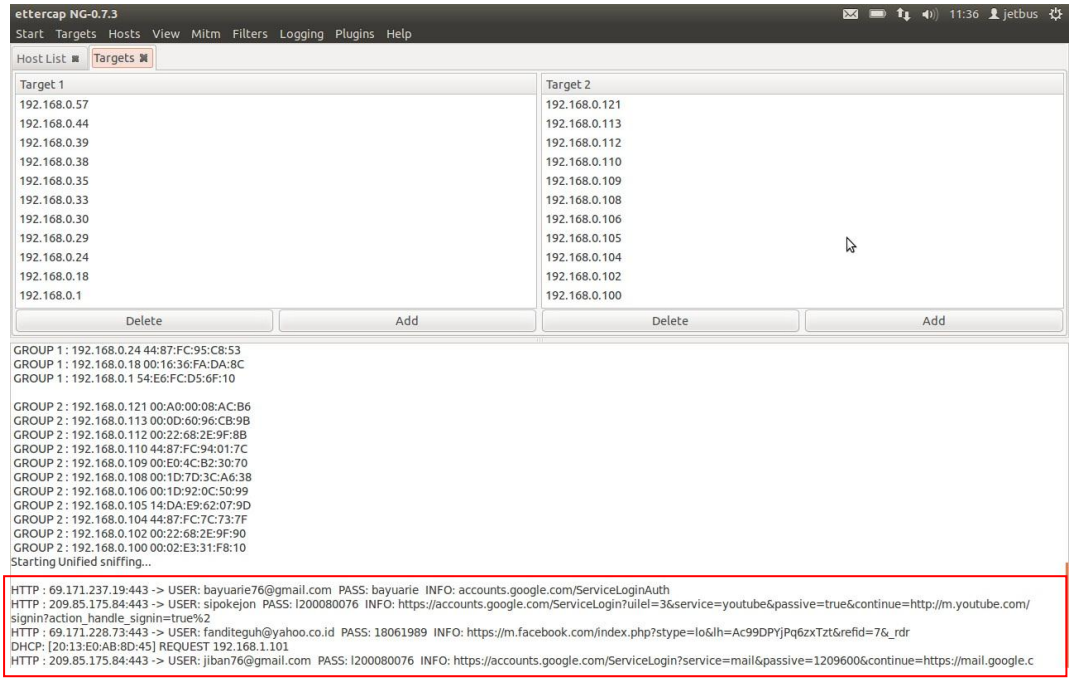
Gambar 4.2. dapat diterangkan bahwa software dapat merekam beberapa aktifitas yang di beri tanda persegi panjang merah, yaitu pada baris 1 s/d 4 sedang terjadi komunikasi pesan antar komputer dengan komputer dalam satu jaringan untuk memastikan bahwa masih terhubung dalam satu jaringan namun tidak terkait oleh pengguna komputer yang artinya pengguna tidak melakukan komunikasi namun secara otomatis mesin komputer mengirim sendiri pesan tersebut yang disebut *ACK (Acknowledgement)*. Kemudian pada baris terakhir menerangkan bahwa ada salah satu komputer *client* yang mengakses akun google mail terekam dengan *username* " bayuarie76@gmail.com "dan *password*-nya " l200080076 ".



Gambar 4.3. Hasil penyerangan Packet Sniffing pada jaringan kabel di kantor TelNav dan Terminal Bandara Adi Sumarmo.

Gambar 4.3. dapat menerangkan bahwa pada baris 1 s/d 13 dalam persegi panjang merah sedang terjadi *file sharing* antara *server* dan *client* namun pesan yang terekam terenkripsi sehingga penulis tidak dapat mendeskripsikannya. Sedangkan pada baris 14 s/d 17 terdapat dua komputer client yang sedang melakukan login akun google mail dengan *username* " jiban76@gmail.com " dan *password* " l200080076 " dan akun yahoo mail dengan *username* " bayuarienugroho@yahoo.co.id " dan *password* " 120989 ".

b. Skenario kedua Penulis mengganti password dan mengacak beberapa akun dan password baru.



Gambar 4.4. Hasil penyerangan Packet Sniffing pada jaringan kabel di gedung baru.

Gambar 4.4. menerangkan bahwa akun yang di ganti password-nya dan beberapa akun dan password yang di acak dapat direkam.

Dari analisis hasil yang didapat penulis mendapatkan pembahasan pihak pengelola jaringan komputer PT. Angkasa Pura I cabang Bandar Udara Internasional Adi Sumarmo dan mendapatkan beberapa alasan mengapa *wifi* pada Kantor TelNav dan Terminal Bandara tidak di beri keamanan atau open, berikut alasannya :

1. *Wifi* yang terinstall di Terminal Bandara merupakan fasilitas bagi pengunjung atau pengguna layanan penerbangan, selagi menunggu jadwal penerbangan atau penjemputan dapat mengakses internet secara mudah dan gratis.
2. *Wifi* yang terinstall di Kantor TelNav merupakan *wifi* utama, ketika suatu saat akan menambah *wifi* lagi tidak sulit untuk mengkonfigurasinya.

Inti dari kedua pembahasan tersebut diatas adalah *wifi* yang terinstall pada PT. Angkasa Pura Bandar Udara Internasional Adi Sumarmo digunakan untuk fasilitas publik tidak untuk di komersilkan jadi

tidak diberi pengamanan seperti WEP, WPA, WPA2 dan lain-lain agar para pengguna jasa layanan penerbangan dapat dengan mudah dan cepat untuk terkonaksi dengan internet.

4.2. PEMBAHASAN

Dari analisis hasil yang didapat penulis mendapatkan pembahasan pihak pengelola jaringan komputer PT. Angkasa Pura I cabang Bandar Udara Internasional Adi Sumarmo dan mendapatkan beberapa alasan mengapa *wifi* pada Kantor TelNav dan Terminal Bandara tidak di beri keamanan atau open, berikut alasannya :

1. *Wifi* yang terinstall di Terminal Bandara merupakan fasilitas bagi pengunjung atau pengguna layanan penerbangan, selagi menunggu jadwal penerbangan atau penjemputan dapat mengakses internet secara mudah dan gratis.

2. *Wifi* yang terinstall di Kantor TelNav merupakan *wifi* utama, ketika suatu saat akan menambah *wifi* lagi tidak sulit untuk mengkonfigurasinya.

Inti dari kedua pembahasan tersebut diatas adalah *wifi* yang terinstall pada PT. Angkasa Pura Bandar Udara Internasional Adi Sumarmo digunakan untuk fasilitas publik tidak untuk di komersilkan jadi tidak diberi pengamanan seperti WEP, WPA, WPA2 dan lain-lain agar para pengguna jasa layanan penerbangan dapat dengan mudah dan cepat untuk terkonaksi dengan internet.

V. KESIMPULAN

Berdasarkan dari analisis data dan percobaan serangan yang dilakukan, maka dapat diambil kesimpulan, bahwa sistem keamanan jaringan *LAN* yang mencakup jaringan kabel dan nirkabel pada PT. Angkasa Pura I Bandar Udara Internasional Adi Sumarmo Surakarta masih perlu peningkatan, hal ini dibuktikan dengan :

1. Aplikasi inSSIDer mendeteksi keamanan *wifi* yang terbuka.

2. Penyerangan *packet sniffing* yang dapat merekam dan menampilkan *username* dan *password* dengan menggunakan aplikasi ettercap.

DAFTAR PUSTAKA

Setiawan, Thomas. 2004. Analisis Keamanan Jaringan Internet Menggunakan Hping, Nmap, Nessus, dan Ethereal. Bandung : Tugas Akhir Institut Teknologi Bandung, (http://budi.insan.co.id/courses/ec5010/projects/thomas-report.pdf, diakses 11 Februari 2012).

Supriyanto, Aji. 2006. Analisis Kelemahan Keamanan Pada Jaringan Wireless. Semarang : Tugas Akhir Universitas Stikubank Semarang, (http://www.unisbank.ac.id/ojs/index.php/fti1/article/download/33/28, diakses 8 Maret 2012).

Noviyanto, Hendri. 2011. Analisis Keamanan Wireless di Universitas Muhammadiyah Surakarta. Surakarta : Tugas Akhir Universitas Muhammadiyah Surakarta.

Sinambela, Josua M. 2007. " Hacking Wifi ", (http://www.te.ugm.ac.id/~josh/seminar/hacking-wifi-josh.pdf, diakses pada tanggal 9 Maret 2012).

Ettercap Home Page. 2012. " Software Ettercap ", (http://ettercap.sourceforge.net, diakses pada tanggal 9 Maret 2012).

Netstumbler Home Page. 2012. " Software Netstumbler ", (http://www.netstumbler.com, diakses pada tanggal 9 Maret 2012).

Metageek Products. 2012. " Software inSSIDer ", (http://www.metageek.net/products/inssider/, diakses pada tanggal 4 April 2012).

Dika. 2012. " Mencegah Arp Poisoning Attack ", (http://bayangannyadika.blogspot.com/2012/04/mencegah-arp-poisoning-attack-dengan.html, diakses pada tanggal 17 Juni 2012).

Oktavianto, Digit. 2012. " Mencegah ARP Spoofing Dan ARP Poisoning Di Linux ", (http://digitoktavianto.web.id/mencegah-arp-spoofing-dan-arp-poisoning-di-linux.html, diakses pada tanggal 19 April 2012).

Fadillah, Fauzan. 2012. " Perancangan dan Analisis Keamanan Jaringan Terhadap ARP Spoofing pada Hotspot ", (http://fauzanfadillah.wordpress.com/2012/02/10/perancangan-dan-analisis-keamanan-jaringan-terhadap-arp-spoofing-pada-hotspot-cont/, diakses pada tanggal 29 Juni 2012).